

DNS Security Market - Forecast from 2026 to 2031

<https://marketpublishers.com/r/DDBB5537353CEN.html>

Date: January 2026

Pages: 145

Price: US\$ 3,950.00 (Single User License)

ID: DDBB5537353CEN

Abstracts

DNS Security Market is projected to increase at a 7.44% CAGR, reaching USD 1.903 billion in 2031 from USD 1.237 billion in 2025.

The DNS (Domain Name System) security market encompasses solutions designed to protect the integrity, availability, and confidentiality of the DNS protocol, a foundational component of internet connectivity. As the internet's address book, DNS is a critical and frequently exploited vector for cyberattacks, making its security essential for organizational resilience. Market growth is driven by the escalating threat landscape, the expansion of digital infrastructure, and the recognition of DNS as both a critical asset to protect and a rich source of threat intelligence.

A primary driver of market expansion is the increasing sophistication and volume of DNS-based attacks. Cybercriminals and advanced threat actors exploit DNS for various malicious activities, including phishing, malware distribution, command-and-control (C2) communication, and data exfiltration. Techniques such as DNS tunneling, cache poisoning, and DNS hijacking are commonly employed to bypass traditional security perimeters. This persistent threat environment compels organizations to implement specialized DNS security solutions that can inspect, filter, and log DNS traffic to detect and block malicious queries before a connection is established, effectively stopping threats at the earliest possible stage.

The widespread adoption of cloud computing and the corresponding shift in network architecture significantly influence the market. Traditional perimeter-based security models are less effective in decentralized, cloud-first environments where users and applications connect directly to the internet. This has accelerated the adoption of cloud-delivered DNS security services. These solutions, often integrated with Secure Web Gateways (SWG) or offered as a standalone DNS-layer security, provide a scalable, flexible, and easily deployable method to enforce security policies for all users and

devices, regardless of location, by routing DNS queries through a secure cloud service for inspection and filtering.

The financial services sector represents a critical and high-demand vertical for DNS security. As a high-value target for financially motivated cybercriminals and state-sponsored actors, the BFSI industry faces relentless threats aimed at disrupting services, stealing sensitive data, and eroding customer trust. DNS-based DDoS attacks, in particular, can cripple online banking and trading platforms. Consequently, financial institutions are prioritizing DNS security as a core component of their cyber defense strategy to ensure service availability, protect customer data, and comply with stringent regulatory requirements for operational resilience.

Increasing regulatory focus and government initiatives are providing additional impetus for market growth. Cybersecurity agencies in various countries are issuing guidelines and advisories highlighting DNS security best practices and the risks associated with its compromise. The introduction of government-sponsored protective DNS services for public sector agencies underscores the strategic importance of securing this layer. Such initiatives raise awareness and set a benchmark for security practices, encouraging broader adoption across both public and private sectors and validating DNS security as a critical control.

A key market challenge is the persistent unpredictability and scale of cyberattacks, including massive, volumetric DDoS attacks that can overwhelm DNS infrastructure. While this threat drives demand, it also places immense pressure on solutions to deliver high performance, low latency, and near-perfect reliability without becoming a bottleneck for legitimate traffic. This performance requirement favors cloud-based providers with globally distributed, anycast networks capable of absorbing large-scale attacks while maintaining service availability.

Geographically, North America maintains a leadership position, driven by early and widespread adoption of advanced cybersecurity solutions, a high concentration of enterprises with mature security postures, and the presence of leading solution vendors. The region's proactive stance on cyber threats, combined with significant investments in IT security across industries, sustains robust demand. Organizations in the region are increasingly leveraging DNS security not only for threat blocking but also for gaining enhanced visibility into network activity and shadow IT usage.

The competitive landscape includes large, diversified network security vendors integrating DNS security into broader platform offerings, as well as specialized providers

focusing on DNS-layer protection and DDoS mitigation. Differentiation is increasingly centered on the quality of threat intelligence—specifically, the ability to leverage real-time, global data to identify and categorize malicious domains—and the integration of artificial intelligence to detect novel threats and anomalous DNS patterns. Seamless integration with existing security ecosystems (SIEM, SOAR, firewalls) for coordinated response is also a critical factor for enterprise adoption.

The DNS security market is evolving from a niche consideration to a fundamental pillar of a modern defense-in-depth strategy. Its growth is inextricably linked to the internet's centrality in business operations and the corresponding need to secure its core protocols. Future market dynamics will be shaped by the continued migration to cloud and hybrid work models, the growing need to secure IoT devices that heavily rely on DNS, and the increasing use of DNS as a proactive sensor for threat hunting. As attacks grow more sophisticated, the role of DNS security in providing early-stage detection and prevention will become even more strategically vital, ensuring its sustained importance within the broader cybersecurity architecture.

Key Benefits of this Report:

Insightful Analysis: Gain detailed market insights covering major as well as emerging geographical regions, focusing on customer segments, government policies and socio-economic factors, consumer preferences, industry verticals, and other sub-segments.

Competitive Landscape: Understand the strategic maneuvers employed by key players globally to understand possible market penetration with the correct strategy.

Market Drivers & Future Trends: Explore the dynamic factors and pivotal market trends and how they will shape future market developments.

Actionable Recommendations: Utilize the insights to exercise strategic decisions to uncover new business streams and revenues in a dynamic environment.

Caters to a Wide Audience: Beneficial and cost-effective for startups, research institutions, consultants, SMEs, and large enterprises.

What do businesses use our reports for?

Industry and Market Insights, Opportunity Assessment, Product Demand Forecasting, Market Entry Strategy, Geographical Expansion, Capital Investment Decisions, Regulatory Framework & Implications, New Product Development, Competitive Intelligence

Report Coverage:

Historical data from 2021 to 2025 & forecast data from 2026 to 2031

Growth Opportunities, Challenges, Supply Chain Outlook, Regulatory Framework, and Trend Analysis

Competitive Positioning, Strategies, and Market Share Analysis

Revenue Growth and Forecast Assessment of segments and regions including countries

Company Profiling (Strategies, Products, Financial Information, and Key Developments among others.

DNS Security Market Segmentation

By Type

DNS Firewall

DNS Servers

Others

By Enterprise Size

Small & Medium Enterprises

Large Enterprises

By End-User

IT & Telecommunication

BFSI

Healthcare

Government

Others

By Geography

North America

United States

Canada

Mexico

South America

Brazil

Argentina

Others

Europe

United Kingdom

Germany

France

Spain

Others

Middle East and Africa

Saudi Arabia

UAE

Others

Asia Pacific

China

Japan

India

South Korea

Australia

Others

Contents

1. EXECUTIVE SUMMARY

2. MARKET SNAPSHOT

- 2.1. Market Overview
- 2.2. Market Definition
- 2.3. Scope of the Study
- 2.4. Market Segmentation

3. BUSINESS LANDSCAPE

- 3.1. Market Drivers
- 3.2. Market Restraints
- 3.3. Market Opportunities
- 3.4. Porter's Five Forces Analysis
- 3.5. Industry Value Chain Analysis
- 3.6. Policies and Regulations
- 3.7. Strategic Recommendations

4. TECHNOLOGICAL OUTLOOK

5. DNS SECURITY MARKET BY TYPE

- 5.1. Introduction
- 5.2. DNS Firewall
- 5.3. DNS Servers
- 5.4. Others

6. DNS SECURITY MARKET BY ENTERPRISE SIZE

- 6.1. Introduction
- 6.2. Small & Medium Enterprises
- 6.3. Large Enterprises

7. DNS SECURITY MARKET BY END-USER

- 7.1. Introduction

- 7.2. IT & Telecommunication
- 7.3. BFSI
- 7.4. Healthcare
- 7.5. Government
- 7.6. Others

8. DNS SECURITY MARKET BY GEOGRAPHY

- 8.1. Introduction
- 8.2. North America
 - 8.2.1. USA
 - 8.2.2. Canada
 - 8.2.3. Mexico
- 8.3. South America
 - 8.3.1. Brazil
 - 8.3.2. Argentina
 - 8.3.3. Others
- 8.4. Europe
 - 8.4.1. United Kingdom
 - 8.4.2. Germany
 - 8.4.3. France
 - 8.4.4. Spain
 - 8.4.5. Others
- 8.5. Middle East and Africa
 - 8.5.1. Saudi Arabia
 - 8.5.2. UAE
 - 8.5.3. Others
- 8.6. Asia Pacific
 - 8.6.1. China
 - 8.6.2. Japan
 - 8.6.3. India
 - 8.6.4. South Korea
 - 8.6.5. Australia
 - 8.6.6. Others

9. COMPETITIVE ENVIRONMENT AND ANALYSIS

- 9.1. Major Players and Strategy Analysis
- 9.2. Market Share Analysis

9.3. Mergers, Acquisitions, Agreements, and Collaborations

9.4. Competitive Dashboard

10. COMPANY PROFILES

10.1. Palo Alto Networks

10.2. Akamai Technologies, Inc.

10.3. EfficientIP

10.4. Mimecast Services Limited

10.5. Cisco

10.6. Open Text Corporation

10.7. Cloudflare Inc.

10.8. Allot Ltd.

10.9. DigiCert

10.10. DNSFilter

11. APPENDIX

11.1. Currency

11.2. Assumptions

11.3. Base and Forecast Years Timeline

11.4. Key Benefits for the Stakeholders

11.5. Research Methodology

11.6. Abbreviations

I would like to order

Product name: DNS Security Market - Forecast from 2026 to 2031

Product link: <https://marketpublishers.com/r/DDBB5537353CEN.html>

Price: US\$ 3,950.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/DDBB5537353CEN.html>